

Weak Secrecy in the Multi-Way Untrusted Relay Channel with Compute-and-Forward

Johannes Richter, Christian Scheunert, Sabrina Engelmann, and
Eduard A. Jorswieck

Abstract

We investigate the problem of secure communications in a Gaussian multi-way relay channel applying the compute-and-forward scheme using nested lattice codes. All nodes employ half-duplex operation and can exchange confidential messages only via an untrusted relay. The relay is assumed to be honest but curious, i.e., an eavesdropper that conforms to the system rules and applies the intended relaying scheme.

We start with the general case of the single-input multiple-output (SIMO) L-user multi-way relay channel and provide an achievable secrecy rate region under a weak secrecy criterion. We show that the securely achievable sum rate is equivalent to the difference between the computation rate and the multiple access channel (MAC) capacity. Particularly, we show that all nodes must encode their messages such that the common computation rate tuple falls outside the MAC capacity region of the relay. We provide results for the single-input single-output (SISO) and the multiple-input single-input (MISO) L-user multi-way relay channel as well as the two-way relay channel. We discuss these results and show the dependency between channel realization and achievable secrecy rate. We further compare our result to available results in the literature for different schemes and show that the proposed scheme operates close to the compute-and-forward rate without secrecy.

This work is supported by the German Research Foundation (DFG) in the Collaborative Research Center 912 “Highly Adaptive Energy-Efficient Computing” and within the Cluster of Excellence “Center for Advancing Electronics Dresden”.

The authors are with the Department of Electrical Engineering and Information Technology, Technische Universität Dresden, 01062 Dresden, Germany. Email: {johannes.richter, sabrina.engelmann, christian.scheunert, eduard.jorswieck}@tu-dresden.de

Index Terms

Physical layer secrecy, multi-way relay channel, network coding, compute-and-forward, lattice codes

I. INTRODUCTION

Network coding has been a promising topic in communications since introduced by Ahlswede et al. in [1]. It was shown that network coding can improve the throughput of a network and achieves the multicast capacity. For static wired networks network coding is very well investigated and some frameworks are developed [2], [3], [4], [5]. On the other hand, there is a lot of ongoing work in the field of network coding for wireless networks. The properties of the wireless channel give the possibility for network coding on different layers. Practical network coding on the forwarding layer has been proposed in [6]. The superposition property of the wireless channel also allows network coding on the physical layer, where the actual network coding is already done by the channel. Physical layer network coding has been investigated in [7] and gained a lot of attention. [8] gives a survey on physical layer network coding techniques. In [9], this approach has been further developed to the compute-and-forward scheme for which the noise is immediately removed at any relay node in the network. This is achieved by decoding linear combinations of incoming symbols at a relay instead of decoding them individually. Compute-and-forward is based on structured codes like lattice codes that have been shown to achieve the additive white Gaussian noise channel capacity with lattice decoding in place of maximum-likelihood decoding in [10].

Beside reliable communication, secrecy considerations have also become more important. Cryptography is based on the currently available computation performance and the time needed to decrypt a message without having the secret key. This kind of security will get weaker with increasing computational power in the years to come. Secrecy on the physical layer offers the possibility that an eavesdropper does not get any information about the exchanged messages. Wyner [11] and Csiszár and Körner [12] proved that confidential data transmission over wiretap channels can be attained by channel coding without secret keys in

terms of weak and strong secrecy, respectively. The achievable secrecy rate in the presence of an untrusted relay is studied in several papers with slightly different scenarios. In [13] Huang et al. investigate different secure transmission schemes in a relay network with a direct connection between source and destination. The question if an untrusted relay is helpful if a direct connection between source and destination exists has been investigated in [14]. In [15] a Gaussian two-hop network is considered where source and destination do not have a direct connection. The destination node can help the source node by jamming the relay node with a random signal. This model is extended in [16] to a multi-hop line network.

The two-way wiretap channel, in which two nodes can only exchange messages via an untrusted relay, was first considered in [17], [18]. It was shown that cooperative jamming, i.e., jamming with controlled interference between codewords, could reduce the eavesdropper's signal-to-noise ratio and hence improve the level of weak secrecy. In [19] it was shown that this result also holds for strong secrecy.

Most secrecy schemes are based on random codes but there is also work done in the field of secrecy through structured codes, namely lattice codes. Achievable rates for the lattice coded Gaussian wiretap channel have been developed in [20]. Theorem 1 in [20] proposes a lattice code construction that achieves the weak secrecy capacity. Lattice codes for the Gaussian wiretap channel have been intensively studied by Oggier et al. in [21] and references therein. They introduced the secrecy gain as a design criterion for good lattice codes for wiretap channels in [22]. It was shown by Ling et al. that lattice codes can achieve strong secrecy over the mod- Λ Gaussian channel [23]. In [24] Ling et al. introduced the flatness factor [25] as the main tool to prove that nested lattice codes can achieve semantic security and strong secrecy over the Gaussian wiretap channel. Compute-and-forward network coding together with strong physical-layer security based on universal hash functions has been investigated in [15]. All these works focus either on a wiretap channel or on a two-hop relay network where a source node transmits via an untrusted relay to a destination. The destination may help by jamming but does not transmit a secure message itself. In [26] Kashyap et al. consider a two-way relay network with an untrusted relay where two nodes transmit one message each

simultaneously via an untrusted relay. They provide an achievable power-rate region with perfect secrecy as well as strong secrecy by applying compute-and-forward.

In this work we consider a L -user relay channel where all users want to securely transmit a message to all other users. There does not exist direct connections between the users and they have to transmit via an untrusted relay which applies compute-and-forward. We investigate the single-input multiple-output (SIMO) multi-way relay channel and provide an achievable weak secrecy rate region. We prove this result and derive results for the single-input single-output (SISO) and multiple-input single-output (MISO) multi-way relay channel as well as the SISO two-way relay channel, which can be seen as special cases of the SIMO multi-way relay channel. Finally, we provide simulation results and compare our scheme against existing schemes.

Our scheme has several advantages over existing schemes. The previous work of [27] and [26] does not consider fading channels and their results can not be easily extended. Our scheme however takes fading into account and uses only well-known techniques like random binning for wiretap channels and compute-and-forward for two-way relaying. Further, we provide an descriptive and convincing interpretation of our result, i.e., the secrecy rate is the compute-and-forward rate region minus the multiple access channel (MAC) rate region. We also achieve a slightly higher secrecy rate when we simplify our model to the model used for example in [27]. A drawback of our scheme is the weak secrecy criterion instead of strong or even perfect secrecy. However, this disadvantage might be overcome by extending our scheme with the same techniques as in [15], namely hashing functions, to provide strong secrecy. This will be part of future work and is not addressed in this paper.

The outline of the paper is as follows. In Section II the system model and the coding scheme are given. Section III provides an achievable secrecy rate region for the L -user SIMO multi-way relay channel. Section IV derives from the previous result the achievable secrecy rate region for the SISO and the MISO multi-way relay channel. Section V investigates the special case of the SISO two-way relay channel. Section VI discusses the results and illustrates them with simulations. Section VII concludes the work.

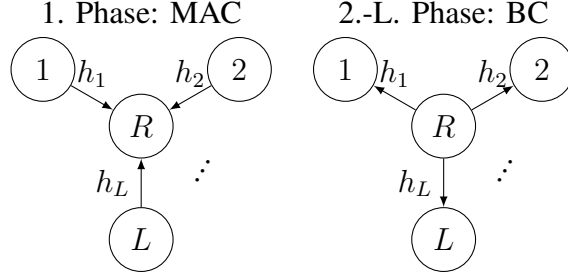


Figure 1: System model: Multi-Way Relay-Channel

A. Notation

Let $\log^+(x) \triangleq \max\{0, \log(x)\}$. We denote by x' the transpose of vector x and by e_i the unit vector with a one at position i and zeros elsewhere. Further we denote by $H(X)$ the entropy of a discrete random variable X and by $h(Y)$ the differential entropy of a continuous random variable Y . The mutual information between two random variables X and Y is denoted by $I(X; Y)$. Let $\mathcal{P}(X)$ be the power set of set X . By $\delta(n)$ we denote a function that tends to zero if n goes to infinity.

II. SYSTEM MODEL

We investigate the multi-way relay-channel with half-duplex nodes as depicted in Figure 1. All nodes have messages for each other but have no direct connection. They transmit messages w_1, \dots, w_L with the help of a relay in L phases. We denote by $x_\ell \in \mathbb{R}^n$ and $x_r \in \mathbb{R}^n$ the transmit signals of the user nodes $1, \dots, L$ and the relay, respectively. Analogously, we define $y_\ell \in \mathbb{R}^n$ and $y_r \in \mathbb{R}^n$ as the received signals at the user nodes and the relay. Each node has a transmit power constraint $\|x_i\|^2 \leq nP, \forall i \in \{1, \dots, L, r\}$. The links are additive white Gaussian noise (AWGN) channels with quasi static block flat fading with fading coefficients h_i and noise z_i with $i \in \{1, \dots, L, r\}$. We assume that the channels are reciprocal and constant over all L phases. This results in the following channel model

$$y_r = \sum_{\ell=1}^L h_\ell x_\ell + z_r, \quad (1a)$$

$$y_\ell = h_\ell x_r + z_\ell. \quad (1b)$$

We consider four scenarios:

- 1) multiple antennas at the relay, which is covered in Section III,
- 2) multiple antennas at the user nodes, which is covered in Section IV,
- 3) single antennas at all nodes, which is covered in Section IV, and
- 4) the two-way relay channel with single antennas at all nodes as a special but important case, which is covered in Section V.

In practice it often happens that such a transmission between nodes has to use a relay that cannot be trusted. Therefore the messages have to be encoded at the source nodes such that the relay cannot decode the messages separately. The reliability requirement at the user nodes $1, \dots, L$ can be written as

$$\lim_{n \rightarrow \infty} \Pr(\hat{w}_\ell \neq w_\ell) = 0, \quad \forall \ell = 1, \dots, L \quad (2)$$

and the weak secrecy requirement as

$$\lim_{n \rightarrow \infty} \frac{1}{n} I(\mathcal{W}; Y_r) = 0, \quad (3)$$

for all $\mathcal{W} \in \mathcal{P}(\{W_1, \dots, W_L\})$ where n is the block length or number of channel uses. For the analysis of the secrecy condition we will also use the following alternative representation of (3)

$$\lim_{n \rightarrow \infty} \frac{1}{n} H(\mathcal{W}) \leq \lim_{n \rightarrow \infty} H(\mathcal{W} | Y). \quad (4)$$

We get the achievable secrecy rates R_{s_1}, \dots, R_{s_L} by choosing $H(W_\ell) = 2^{nR_{s_\ell}}$ such that

$$\lim_{n \rightarrow \infty} \frac{1}{n} \log_2 H(W_\ell) = R_{s_\ell}. \quad (5)$$

Because the relay is the intended receiver of the messages and the eavesdropper at the same time, some additional effort is needed to ensure secret message transmission. We can already see, that we can achieve this condition only if we apply a relaying scheme where the relay does not need to decode the single messages. Further we need to achieve a transmission rate larger than the MAC capacity otherwise the relay would be able to decode the single messages. This is a necessary but not a sufficient condition. A relaying strategy which allows to fulfill these requirements is compute-and-forward, which was introduced by Nazer and Gastpar in [9]. We will use this framework to provide an achievable secrecy rate region.

A. Nested Lattice Code

The compute-and-forward framework is based on nested lattice codes and therefore we recall some lattice definitions that are used throughout the paper. For further details on lattice codes see [28], [29], [8], [30].

An n -dimensional lattice $\Lambda \subset \mathbb{R}^n$ is a group under addition with generator matrix $G \in \mathbb{R}^{n \times n}$.

$$\Lambda = \{Gc : c \in \mathbb{Z}^n\}. \quad (6)$$

A lattice quantizer is a mapping $Q_\Lambda : \mathbb{R}^n \rightarrow \Lambda$ that maps a point x to the nearest lattice point in Euclidean distance,

$$Q_\Lambda(x) = \arg \min_{\lambda \in \Lambda} \|x - \lambda\|. \quad (7)$$

Let the modulo operation with respect to the lattice Λ be defined as

$$x \bmod \Lambda = x - Q_\Lambda(x). \quad (8)$$

We call $\mathcal{V} = \{x : Q_\Lambda(x) = 0\}$ the fundamental Voronoi region of the lattice Λ and denote by $\text{Vol}(\mathcal{V})$ the volume of \mathcal{V} . Two lattices Λ_C and Λ_F are called nested, if $\Lambda_C \subseteq \Lambda_F$. We call Λ_C the coarse lattice and Λ_F the fine lattice. A nested lattice code \mathcal{L} is formed by taking all of the points of the fine lattice Λ_F in the fundamental Voronoi region \mathcal{V}_C of the coarse lattice Λ_C , i.e., $\mathcal{L} = \Lambda_F \cap \mathcal{V}_C$. The rate of a nested lattice code is given by

$$r = \frac{1}{n} \log |\mathcal{L}| = \frac{1}{n} \log \frac{\text{Vol}(\mathcal{V}_C)}{\text{Vol}(\mathcal{V}_F)}. \quad (9)$$

From [10] and [30] we know that there exist good nested lattice codes that can achieve the capacity of an AWGN channel. These nested lattice codes have been used to develop the compute-and-forward framework [9], [8]. We utilize this framework as relaying strategy and extend it with secrecy constraints as described above.

B. Encoding

Each user node ℓ chooses a message $w_\ell \in \mathbb{F}_p^k$ i.i.d. from a uniform distribution over the index set $\{1, 2, \dots, 2^{\lfloor nR_s \rfloor}\}$. For the ease of simplicity we assume equal message length at

all users. If this is not the case, messages with length smaller than k will be padded to length k with zeros. Each message gets mapped to a lattice code $\mathcal{L} = \Lambda_F \cap \mathcal{V}_C$ where the second moment of Λ_C equals P such that the power constraint is satisfied. In order to fulfill the secrecy requirements some additional effort is required. Each user node ℓ uses the same codebook $\mathcal{L} = \Lambda_F \cap \mathcal{V}_C$ with $|\Lambda_F \cap \mathcal{V}_C| = 2^{\lfloor n(R_s + R_d) \rfloor}$. Like wiretap codes, this codebook is randomly binned into several bins, where each bin contains $2^{\lfloor nR_d \rfloor}$ codewords. The secret message w_ℓ gets mapped to the bins. The actual transmitted codeword t_ℓ is chosen from that bin according to a uniform distribution.

Further we add some dither u_ℓ that is uniform distributed over \mathcal{V}_C and known by the relay. This dithering gives statistical properties of the transmitted signal needed to achieve the compute-and-forward rate [9]. It was shown in [9, Appendix C] that this dither might be chosen in a deterministic way. To make sure that the transmit signal fulfills the power constraint, we build the modulo with respect to the coarse lattice. We get the following n -dimensional transmit vector at node ℓ

$$x_\ell = [t_\ell + u_\ell] \bmod \Lambda_C. \quad (10)$$

With this encoding scheme we get the following rates:

- a) R_d is the rate of the randomly chosen messages within a bin,
- b) R_s is the secret message rate, and
- c) $R_s + R_d = \frac{1}{n} \log_2 \frac{\text{Vol}(\mathcal{V}_C)}{\text{Vol}(\mathcal{V}_F)}$ is the transmit rate of the user nodes.

III. SIMO MULTI-WAY RELAY CHANNEL

In the following section we investigate the SIMO channel, i.e., the relay is equipped with multiple antennas. The system model for the first phase from the user nodes to the relay is shown in Figure 2. We want to point out, that this is the most general case without assuming multiple-input multiple-output (MIMO) channels because the SISO and MISO channel can be seen as special cases as described later.

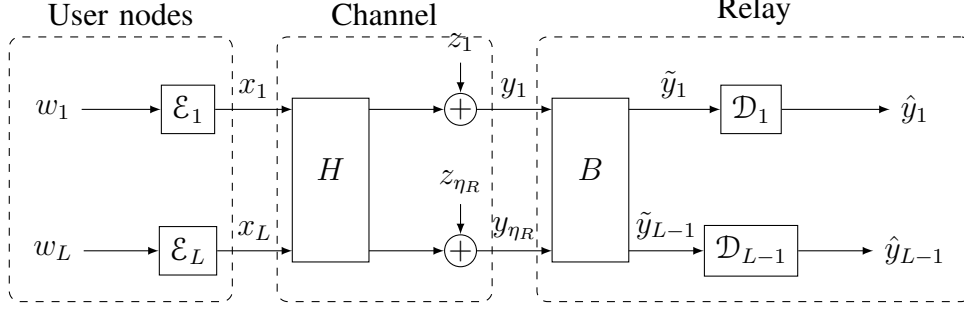


Figure 2: System model of a SIMO L -user relay channel (MAC phase)

A. Channel Model

We assume the relay is equipped with η_R antennas and therefore receives η_R signals y_1, \dots, y_{η_R} . The channel is characterized by the channel matrix $H \in \mathbb{R}^{\eta_R \times L}$ whose entries h_{ij} are the fading coefficients from the j -th user to the i -th antenna at the relay. Note that by this representation the i -th row of H , denoted by h_i , represents the channel from user i to the relay. The channel model for the first phase is then given by

$$Y = HX + Z, \quad (11)$$

where $X \in \mathbb{R}^{L \times n}$ is a matrix whose i -th row is the transpose transmit vector x'_i of user i . Further, $Y \in \mathbb{R}^{\eta_R \times n}$ is a matrix whose i -th row represents the received data stream y'_i at the i -th antenna and $Z \in \mathbb{R}^{\eta_R \times n}$ is white Gaussian noise. The rows of Z are denoted by z_i and are i.i.d. according to a normal distribution with zero mean and unit variance, i.e., $z_i \sim \mathcal{N}(0, I_n)$. The relay decodes $L - 1$ linear combinations of the original messages and encodes them with a capacity achieving code. The $L - 1$ codewords are then sent to all users simultaneously in the remaining $L - 1$ phases. Note that for these phases we have a broadcast channel and we assume reciprocal channels which are constant over all L phases. Therefore the rate constraints for the last $L - 1$ phases are given by the capacity of the individual point-to-point channels. Due to the uplink-downlink duality for reciprocal channels and equal power constraints [31, Chapter 10.3], these are always larger or equal to the MAC rate region and the first phase will be the limiting phase. Therefore we will focus on that phase for developing the achievable rate of the whole system.

B. Relay Strategy

The relay uses compute-and-forward [9] as relaying strategy and tries to decode $L - 1$ linear combination of the original messages as shown in Figure 2. It uses a preprocessing matrix B to get the optimal signals prior to decoding. The achievable computation rate is then given by [9], [32]

$$R(H, a_\ell, b_\ell) = \frac{1}{2} \log_2 \left(\frac{P}{\|b_\ell\|^2 + P\|H'b_\ell - a_\ell\|^2} \right), \quad (12)$$

where a_ℓ is the coefficient vector for the ℓ -th linear combination and b_ℓ is the preprocessing vector corresponding to the ℓ -th row in B . The optimal preprocessing matrix for a given coefficient matrix $A = (a'_1, \dots, a'_{L-1})'$ and the resulting rates have been found in [32]. We use these results and provide them in the following for completeness.

The optimal preprocessing matrix is given by

$$B = AH'(HH' + \frac{1}{P}I_{\eta_R})^{-1}. \quad (13)$$

Plugging in (13) in (12), we get

$$R(H, a_\ell) = -\frac{1}{2} \log_2(a'_\ell V D V' a_\ell), \quad (14)$$

where $V \in \mathbb{R}^{L \times L}$ is the right eigenmatrix of H and $D \in \mathbb{R}^{L \times L}$ is a diagonal matrix with elements

$$D_{ii} = \begin{cases} \frac{1}{P\lambda_i + 1} & i \leq \text{rank}(H) \\ 1 & i > \text{rank}(H) \end{cases}, \quad (15)$$

where λ_i is the i -th eigenvalue of $H'H$.

All $L - 1$ linear combinations have to be decodable at the relay to allow all L users to decode all original messages. Therefore the resulting achievable rate of all L users is

$$R_{CF} = \min_{\ell \in \{1, \dots, L-1\}} R(H, a_\ell). \quad (16)$$

To get the highest possible rates we need to find a set of full rank equations with coefficient matrix $A \in \mathbb{Z}^{L-1 \times L}$. Because all L users need to be able to decode all messages, we additionally require the rows of A to be linear independent of all vectors e_ℓ where e_ℓ is the

unit vector with a one at the ℓ -th position and zeros elsewhere. This results in the following optimization problem

$$\begin{aligned} \max_{A_\ell} \min_{\ell \in \{1, \dots, L-1\}} & \left(-\frac{1}{2} \log_2(a'_\ell V D V' a_\ell) \right) \\ \text{s.t. } & \text{rank}(A_\ell) = L, \forall i \in \{1, \dots, L\} \end{aligned} \quad (17)$$

where

$$A_\ell = \begin{pmatrix} a'_1 \\ \vdots \\ a'_{L-1} \\ e'_\ell \end{pmatrix} = \begin{pmatrix} a_{1,1} & a_{1,2} & \dots & a_{1,L} \\ \vdots & \vdots & \ddots & \vdots \\ a_{L-1,1} & a_{L-1,2} & \dots & a_{L-1,L} \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

This can be solved by several algorithms [33], [34] with additional constraints.

For the first phase we get the following rate constraint

$$R_s + R_d \leq R_{CF}. \quad (18)$$

In the second phase the relay maps all decoded linear combinations $\hat{y}_i \in \Lambda_F \cap \mathcal{V}_C$ to an index of the set $\{1, 2, \dots, 2^{\lfloor nR_r \rfloor}\}$ and uses a capacity achieving code to encode and an optimal beamforming vector to transmit to the user nodes with rate

$$R_r = \max_{\|\omega\|^2 \leq 1} \min_{\ell \in \{1, \dots, L\}} \frac{1}{2} \log_2(1 + P(\omega' h_\ell)^2), \quad (19)$$

where ω is the multicast beamforming vector at the relay. An efficient way to obtain the optimal beamforming vector can be found in [35].

C. Decoding at the user nodes

In each of the $L - 1$ phases, each user node receives an index of the set $\{1, 2, \dots, 2^{\lfloor nR_r \rfloor}\}$. They can decode as long as the transmission rate from relay to user is less than the point-to-point capacity of the channels, which is given in (19). If decoded successfully they know the lattice point $\hat{y}_\ell \in \Lambda_F \cap \mathcal{V}_C$ being transmitted by the relay.

User ℓ can decode the original lattice points from the other users by solving the following system of linear equations

$$A_\ell T = \tilde{Y}_\ell \quad (20)$$

where

$$\tilde{Y}_\ell = \begin{pmatrix} \hat{y}_{1,1} & \hat{y}_{1,2} & \cdots & \hat{y}_{1,n} \\ \vdots & \vdots & \ddots & \vdots \\ \hat{y}_{L-1,1} & \hat{y}_{L-1,2} & \cdots & \hat{y}_{L-1,n} \\ t_{\ell,1} & t_{\ell,2} & \cdots & t_{\ell,n} \end{pmatrix}. \quad (21)$$

It gets an estimate of the transmitted lattice points t_ℓ of the users $1, \dots, L$ by

$$\hat{T}_\ell = A_\ell^{-1} \tilde{Y}_\ell. \quad (22)$$

User ℓ already knows t_ℓ because this is its own message. Please note that the users get the lattice points without the dither because the relay already subtracted it.

After solving for T_ℓ each user knows all L lattice point. If the lattice point is known, the message and the bin is known. Therefore each user gets all L messages.

From all L phases we obtain a rate constraint for the source nodes given by

$$R_d + R_s \leq \min\{R_{CF}, R_r\} = R_{CF}. \quad (23)$$

From the lattice code construction in Section II-A and (23) we get the following constraint for the secure communication rate R_s

$$R_s \leq R_{CF} - R_d. \quad (24)$$

We get the same constraint for all source nodes because all use the same nested lattice chain. To ensure that the relay will not get any information about individual messages, the rate R_d has to be chosen appropriately. This will be addressed in the next section.

D. Achievable Secrecy Rate Region

In this section we provide an achievable secrecy rate region. The proof is given in the appendix.

Theorem 1 (Achievable Secrecy Rate). *Consider a multi-way relay channel with L users and η_R antennas at the relay. The channel is characterized by the matrix H whose entries h_{ij} represent the fading coefficient from the j -th user to the i -th antenna at the relay. All*

nodes can only communicate via the relay and have no direct links. Each node has a transmit power constraint $\|x_i\|^2 \leq nP$, $\forall i \in \{1, \dots, L, r\}$. Then the weak secrecy rate region is given by

$$L \cdot R_s \leq \max \left\{ 0, LR_{CF} - \frac{1}{2} \log_2 \det(I_{\eta_R} + PHH') \right\}$$

where

$$R_{CF} = \min_{i \in \{1, \dots, L-1\}} R(H, a_i)$$

with a_i chosen in programming problem (17).

E. Power Allocation

Every source node has a power constraint $\|x_\ell\| \leq nP$. However, it is not always optimal to send at full power and therefore the transmit power for each source node needs to be optimized. We define a diagonal matrix $P_{\text{tr}} = \text{diag}(\sqrt{P_1}, \dots, \sqrt{P_L})$ which contains the square roots of the individual transmit powers of the source nodes. Further, we define the effective channel as $\tilde{H} = HP_{\text{tr}}$. This results in the following optimization problem

$$\max_{P_\ell \leq P} LR_{CF} - \frac{1}{2} \log_2 \det(I_{\eta_R} + HP_{\text{tr}}P_{\text{tr}}'H'), \quad (25)$$

where

$$R_{CF} = \min_{\ell \in \{1, \dots, L-1\}} -\frac{1}{2} \log_2(a_\ell'VDV'a_\ell), \quad (26)$$

where V is the right singular matrix of \tilde{H} and D is a diagonal matrix with elements

$$D_{ii} = \begin{cases} \frac{1}{\lambda_i+1} & i \leq \text{rank}(\tilde{H}) \\ 1 & i > \text{rank}(\tilde{H}) \end{cases}, \quad (27)$$

where λ_i is the i -th eigenvalue of $\tilde{H}'\tilde{H}$.

This problem is hard to solve because of the non-linearity and non-convexity. The scope of this paper does not include an analytic result or an algorithm. For the simulations we use a grid search algorithm to obtain the optimal power allocation.

IV. SISO AND MISO MULTI-WAY RELAY CHANNEL

In this section we provide the achievable secrecy rates for the following cases:

- single antenna at the source nodes and the relay; SISO,
- multiple antennas at the source nodes and single antenna at the relay; MISO.

These can be written as special cases of the SIMO case.

A. SISO

The results for the SISO case can be derived directly from Theorem 1 where the channel matrix reduces to a vector.

Corollary 1. *Consider a multi-way relay channel with L users and single antennas at all nodes. The channel from user ℓ to the relay is characterized by the coefficient $h_\ell \in \mathbb{R}$ with $h = (h_1, \dots, h_L)'$. All nodes can only communicate via the relay and have no direct links. Each node has a transmit power constraint $\|x_i\|^2 \leq nP$, $\forall i \in \{1, \dots, L, r\}$. Then the weak secrecy rate region is given by*

$$L \cdot R_s \leq \max \left\{ 0, LR_{CF} - \frac{1}{2} \log_2(1 + \|\tilde{h}\|^2) \right\}$$

where

$$R_{CF} = \min_{i \in \{1, \dots, L-1\}} \log_2^+ \left(\left(\|a_i\|^2 - \frac{(\tilde{h}'a_i)^2}{1 + \|\tilde{h}\|^2} \right)^{-1} \right).$$

Further, $\tilde{h} = \text{diag}(\sqrt{P_1}, \dots, \sqrt{P_L}) \cdot h$ is the effective channel and $P_\ell \leq P$ is the transmit power at user ℓ .

B. MISO

For the MISO case we assume no cooperation at the source nodes for choosing the beamforming vectors. Therefore it is optimal to use maximum ratio transmission (MRT) in the direction of the channel. This leaves us with an reduced optimization problem where we only have to choose the optimal power allocation. The effective channel is

$$\tilde{h} = \text{diag}(\sqrt{P_1}, \dots, \sqrt{P_L}) \cdot (h'_1 \omega_1, \dots, h'_L \omega_L)', \quad (28)$$

where h_ℓ is the channel vector from user ℓ to the relay and ω_ℓ is the beamforming vector with $\|\omega_\ell\| \leq 1$ for user ℓ . Using MRT we get

$$\omega_\ell = \frac{h_\ell}{\|h_\ell\|} \text{ and } h'_\ell \omega_\ell = \|h_\ell\|. \quad (29)$$

The secrecy rate is now equivalent to the one in the SISO case and we get the following corollary.

Corollary 2. *Consider a multi-way relay channel with L users and η_T antennas at the user nodes. The relay is equipped with a single antenna. The channel from user ℓ to the relay is characterized by the vector $h_\ell \in \mathbb{R}^{\eta_T}$. All nodes can only communicate via the relay and have no direct links. Each node has a transmit power constraint $\|x_i\|^2 \leq nP$, $\forall i \in \{1, \dots, L, r\}$. Then the weak secrecy rate region is given by*

$$L \cdot R_s \leq \max \left\{ 0, LR_{CF} - \frac{1}{2} \log_2(1 + \|\tilde{h}\|^2) \right\}$$

where

$$R_{CF} = \min_{i \in \{1, \dots, L-1\}} \log_2^+ \left(\left(\|a_i\|^2 - \frac{(\tilde{h}' a_i)^2}{1 + \|\tilde{h}\|^2} \right)^{-1} \right).$$

Further, $\tilde{h} = \text{diag}(\sqrt{P_1}, \dots, \sqrt{P_L}) \cdot (\|h_1\|, \dots, \|h_L\|)'$ is the effective channel and $P_\ell \leq P$ is the transmit power at user ℓ .

V. 2-USER CASE: TWO-WAY RELAY CHANNEL

In this section we consider the special case of two users which is also known as the two-way relay channel. We restrict ourselves to the SISO case where all nodes are equipped with single antennas. This system model is quite common in literature and one can find a lot of work on the achievable rate without secrecy [36], [37], [38] as well as with secrecy [17], [19], [15], [39], [40]. Most of the work models the two-way relay channel as a wiretap channel where the second user is helping the first user by jamming the eavesdropper, i.e., the relay [27], [41]. This differs from our work because we assume that both users transmit a secure message simultaneously. Further, most of the work so far considers the two-way relay channel without fading and those results cannot be directly extended to fading channels.

However, to be able to compare our result to existing schemes we relax our model to match the one assumed in [27]. That is, user 1 transmits a secure message to user 2 via an untrusted relay. User 2 helps by sending a jamming signal to the relay. The main difference to our more general model is the fact, that the message of the second user does not need to be secure. Further, we assume that the channel coefficients are equal and set to 1. With this relaxed model we get the following secrecy rate.

Theorem 2. *Consider a two-way relay channel with fading coefficients $h_1 = h_2 = 1$ and equal power constraint P . The following secrecy rate is achievable with a cooperative jammer*

$$\begin{aligned} R_s &\leq \max \left\{ 0, \frac{1}{2} \log_2 \left(\frac{1}{2} + P \right) - \frac{1}{2} \log_2 \left(1 + \frac{P}{1+P} \right) \right\} \\ &= R_s^{CF}. \end{aligned}$$

Proof: The following proof does not necessarily require that the channel fading coefficients are 1. Therefore we provide the proof with fading coefficients and choose them to be 1 at the end to get result of Theorem 2. The proof follows the same steps as the proof for the L -user multi-way relay channel, except that we have only the following secrecy requirement:

$$\lim_{n \rightarrow \infty} \frac{1}{n} H(W_1 | Y_r) \geq \lim_{n \rightarrow \infty} \frac{1}{n} H(W_1) = R_s. \quad (30)$$

We start by bounding the conditional entropy of the message W_1 given the received signal Y_r at the relay,

$$H(W_1 | Y_r) \quad (31)$$

$$= H(W_1 | X_1, Y_r) + H(X_1 | Y_r) - H(X_1 | W_1, Y_r) \quad (32)$$

$$\geq H(X_1 | Y_r) - n\delta(n) \quad (33)$$

$$= H(X_1 | Y_r) - H(X_1) + H(X_1) - n\delta(n) \quad (34)$$

$$= H(X_1) - I(X_1; Y_r) - n\delta(n), \quad (35)$$

where we used Fano's inequality to bound the last term in (32). This is because the size of each bin is kept small enough such that given W_1 , the eavesdropper/the relay can determine

X_1 from its received signal Y_r [27].

We now need a lower bound on the mutual information between X_1 and Y_r .

$$I(X_1; Y_r) \tag{36}$$

$$= h(Y_r) - h(Y_r | X_1) \tag{37}$$

$$\leq n \cdot \frac{1}{2} \log_2(2\pi e(Ph_1^2 + Ph_2^2 + 1)) - h(h_2X_2 + Z_r) \tag{38}$$

The last inequality follows from the fact that a normal distribution maximizes the entropy under an average power constraint. The last term can be expressed as follows,

$$h(h_2X_2 + Z_r) \tag{39}$$

$$= h(h_2X_2 + Z_r | h_2X_2) + I(h_2X_2; h_2X_2 + Z_r) \tag{40}$$

$$= h(Z_r) + I(h_2X_2; h_2X_2 + Z_r), \tag{41}$$

where $h(Z_r) = \frac{1}{2} \log_2(2\pi e)$. From [10] we know that

$$\lim_{n \rightarrow \infty} \frac{1}{n} I(h_2X_2; h_2X_2 + Z_r) = \frac{1}{2} \log_2(1 + h_2^2 P). \tag{42}$$

If we combine (38), (41) and (42) we get

$$\lim_{n \rightarrow \infty} \frac{1}{n} H(X_1 | Y_r) \tag{43}$$

$$\geq \lim_{n \rightarrow \infty} \frac{1}{n} [H(X_1) - I(X_1; Y_r) - n\delta(n)] \tag{44}$$

$$\geq \lim_{n \rightarrow \infty} \frac{1}{n} [H(X_1) - n \cdot \frac{1}{2} \log_2(2\pi e(h_1^2 P + h_2^2 P + 1)) + h(Z_r) + I(h_2X_2; h_2X_2 + Z_r)] \tag{45}$$

$$= (R_s + R_d) - \frac{1}{2} \log_2(h_1^2 P + h_2^2 P + 1) + \lim_{n \rightarrow \infty} \frac{1}{n} I(h_2X_2; h_2X_2 + Z_r) \tag{46}$$

$$= (R_s + R_d) - \frac{1}{2} \log_2 \left(1 + \frac{h_1^2 P}{1 + h_2^2 P} \right) \tag{47}$$

Because $R_s + R_d \leq R_{\text{CF}}$ we get the following result,

$$R_s \leq R_{\text{CF}} - \frac{1}{2} \log_2 \left(1 + \frac{h_1^2 P}{1 + h_2^2 P} \right). \tag{48}$$

Choosing $h_1 = h_2 = 1$ we get the result of Theorem 2. This concludes the proof. ■

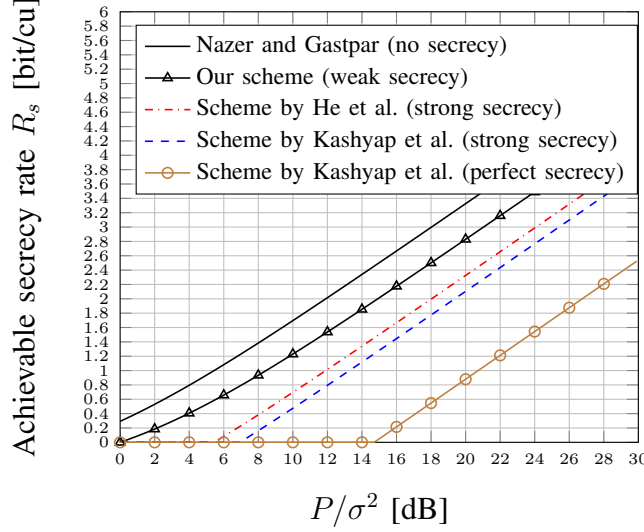


Figure 3: Achievable secrecy rate of the two-way relay channel with $h = (1, 1)'$ and $\sigma^2 = 1$ for different schemes.

In the following we compare our result for the two-way relay channel to other approaches and illustrate the results in Figure 3. The first result is a scheme by He and Yener which provides a weak secrecy result [27], i.e.,

$$R_s \leq \max\{0, \frac{1}{2} \log_2(\frac{1}{2} + P) - 1\} = R_s^{\text{HS}}. \quad (49)$$

This result is extended in [15] for strong secrecy. The achievable secrecy rate is shown to be the same as for weak secrecy by utilizing a hash function. Please note that we can extend our result as well with a hash function to get a result for strong secrecy. This will be the topic of future research and is not considered in this paper.

The second scheme is provided by Kashyap et al. in [26]. The achievable secrecy rates are

$$R_s \leq \max\{0, \frac{1}{2} \log_2(P) - 1 - \log_2(e)\} = R_s^{\text{KP}} \quad (50)$$

and

$$R_s \leq \max\{0, \frac{1}{2} \log_2(\frac{1}{2} + P) - \log_2(2e)\} = R_s^{\text{KS}} \quad (51)$$

for perfect and strong secrecy, respectively. Observe that $R_{\text{CF}} \geq R_s^{\text{CF}} \geq R_s^{\text{HS}} \geq R_s^{\text{KS}} \geq R_s^{\text{KP}}$.

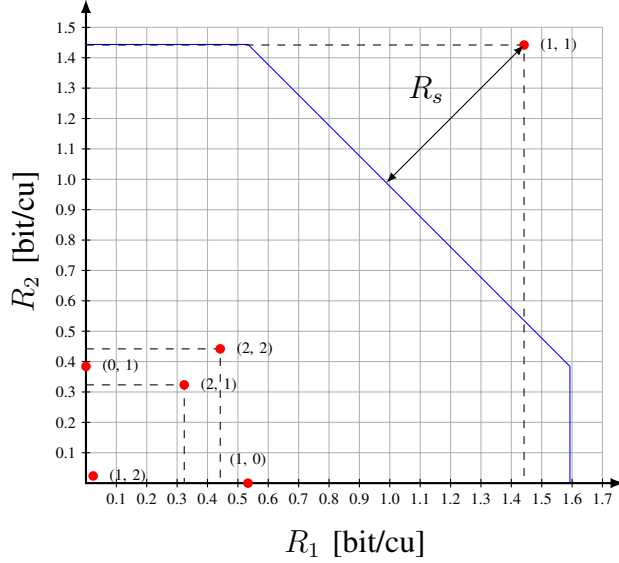


Figure 4: MAC capacity region (blue line) with achievable compute-and-forward rates for different coefficient vectors a (red dots) for $h = (0.9, 0.8)'$ and $P = 10$ Watt.

VI. DISCUSSION

In this section we discuss and illustrate Theorem 1, Corollary 1 and Corollary 2. It is interesting to note, that the achievable secrecy rate is the difference between the achievable compute-and-forward sum rate and the sum capacity of the MAC. This means, we get a secrecy rate greater than zero if the compute-and-forward rate region is larger than the MAC capacity region. This is illustrated in Figure 4 for the two user case, where we plotted the achievable rate regions for the channel coefficients $(0.9, 0.8)'$ and a transmit power constraint of $P = 10$ Watt. The dots in Figure 4 mark the corner points of the achievable compute-and-forward rate regions for different linear combinations. The solid line illustrates the border of the MAC capacity region. As one can see, a rate greater than the MAC sum capacity is only achievable for a single coefficient vector, in this example $a = (1, 1)'$. In general there can be at most one point or several linear dependent points outside the MAC capacity region. Otherwise the relay would be able to decode the single messages by solving a system of linear equations which contradicts the MAC capacity definition. From this illustration we see, that it is only possible to transmit secure messages via the relay, if the source nodes

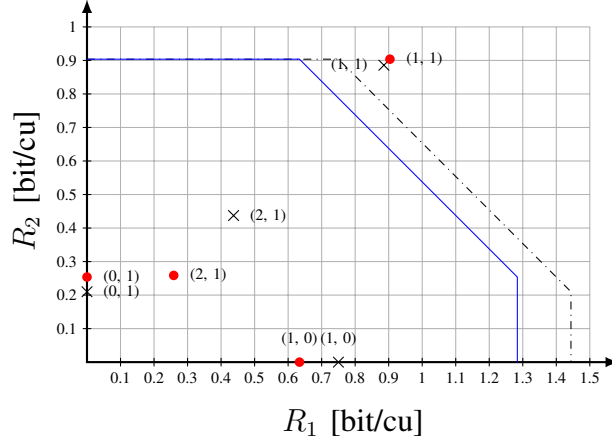


Figure 5: MAC capacity region with achievable compute-and-forward rates for different coefficient vectors a at full transmit power (dashdotted line and crosses) and at optimal transmit power (7.7, 10.0) Watt (blue solid line and red dots) for $h = (0.8, 0.5)'$ and $P = 10$ Watt.

transmit at a rate outside the MAC capacity. This ensures that the relay cannot decode the single messages but only a linear combination, if the compute-and-forward rate is higher than the MAC sum capacity. In Figure 4 it is optimal to transmit at full power. In Figure 5 we show that this is not always the case. Therefore we plotted the achievable rate regions for the channel coefficients $(0.8, 0.5)'$ and a transmit power constraint of $P = 10$ Watt. As one can see optimizing the power means reducing the transmit power for one user node. Because the channel coefficients of the effective channel are then closer to each other, we achieve a higher computation rate for the coefficient $a = (1, 1)'$ while reducing the MAC sum capacity at the same time. We want to stress here the not common behavior that it is possible to increase the secrecy rate by reducing the transmit power.

A. Achievability Of Positive Secrecy Rates

The achievable compute-and-forward sum rate is the double of the computation rate at the relay. The achievable computation rate depends highly on the channel coefficients because the compute-and-forward framework tries to approximate the real valued channel coefficients with integer valued network coding coefficients. This means that there does not always exist a

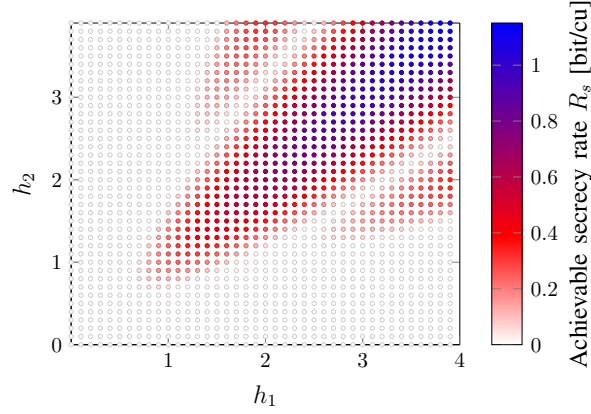


Figure 6: Existence of a compute-and-forward rate tuple outside of the multiple access channel capacity region. $P/\sigma^2 = 5\text{dB}$.

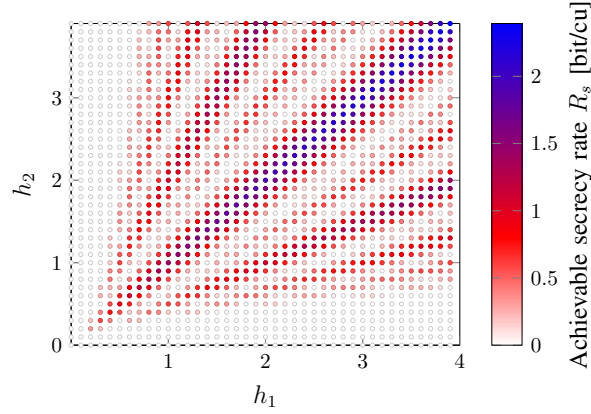


Figure 7: Existence of a compute-and-forward rate tuple outside of the multiple access channel capacity region. $P/\sigma^2 = 20\text{dB}$.

network coding coefficient vector with an achievable computation rate which is larger than the MAC capacity. We show in Figure 6 and Figure 7 the achievable secrecy rate for different channel realizations in a two user scenario, i.e., the two-way relay channel with a single antenna at all nodes. One can see that the achievable secrecy rate reaches its highest values if the channel coefficients are equal. One can also see that small channel coefficient values do not achieve positive secrecy rates. One can compensate this behavior in part by adjusting the power allocation such that the effective channel coefficients are close to each other. Unfortunately, when we assume that the channel coefficients are distributed by $h_i \sim \mathcal{N}(0, 1)$,

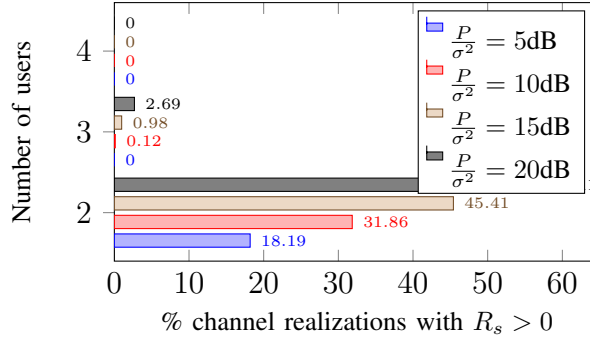
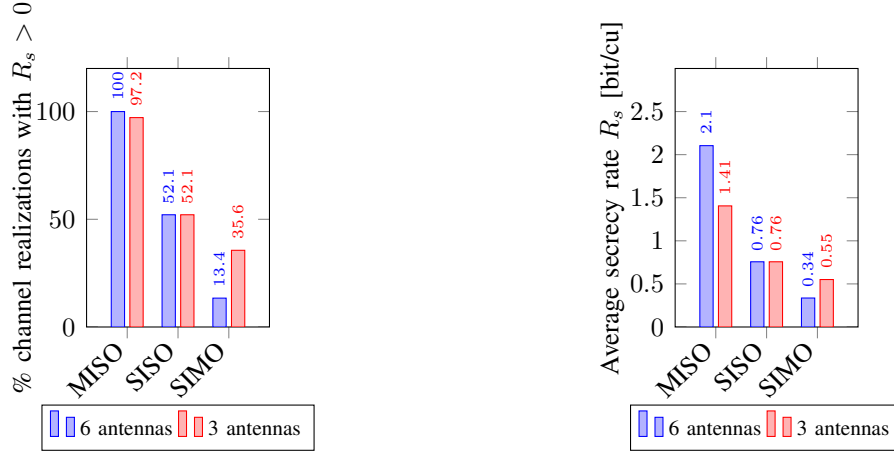


Figure 8: Percentage of channel realizations resulting in positive secrecy rates for different numbers of users and SNR values for the SISO multi-way relay channel without optimal power allocation. 10,000 channel realizations are drawn from a normal distribution $\mathcal{N}(0, 1)$.

the small channel coefficients occur with higher probability. The question arises how many channel realizations result in a positive secrecy rate when we draw the channel coefficients from a normal distribution with zero mean and unit variance. The result for the SISO case without optimized power allocation is shown in Figure 8 where we used 10,000 i.i.d. channel realizations. One can see that only in the two-way relay channel we achieve positive secrecy rates for a reasonable amount of channel realizations. This might be a depressing result but we can do better by optimizing the transmit power and introducing multiple antennas. The result for a signal-to-noise ratio (SNR) of 5dB is shown in Figure 9. One can see that alone by optimizing the power allocation in the SISO case we increase the channel realizations resulting in a positive secrecy rate from 18.19% to 52.1%. Introducing multiple antennas at the source nodes results in 100% of positive secrecy rates. Introducing multiple antennas at the relay is contra-beneficial because we give the eavesdropper more degrees of freedom.

VII. CONCLUSION

In this paper we have presented an achievable secrecy rate region for the L-user relay channel where all nodes want to securely transmit messages via an untrusted relay. We have shown that the proposed coding strategy, based on the compute-and-forward framework, supports simultaneous secure communications. The proposed achievable secrecy rate is the



(a) Percentage of channel realizations resulting in positive secrecy rates (b) Average secrecy rate over all positive rates

Figure 9: Percentage of channel realizations resulting in positive secrecy rates and the according average secrecy rates for $P/\sigma^2 = 5\text{dB}$. All schemes use optimal power allocation. 1000 channel realizations are drawn from a normal distribution $\mathcal{N}(0, 1)$.

difference between the MAC sum capacity and the computation rate of the compute-and-forward framework. We have provided a proof for the achievability of the secrecy rate region and have discussed this result. We have seen that this scheme performs quite good in the 2-user case, commonly known as the two-way untrusted relay channel. Therefore we investigated this scenario in detail and showed the dependency of the performance on the channel realizations. We showed that by introducing multiple antennas at the source nodes and optimizing the transmit power we can significantly increase the secrecy rate.

ACKNOWLEDGMENT

The authors would like to thank Martin Mittelbach from the Department of Electrical Engineering and Information Technology at Technische Universität Dresden for valuable discussions.

Table I: Overview of variables and symbols

variable	distribution	comment
W_i	$\sim \mathcal{U}(\{1, 2, \dots, \lceil 2^{nR_s} \rceil\})$	secret message of length k
U_i	$\sim \mathcal{U}(\mathcal{V}_C)$	dither at node i
X_i	$\sim \mathcal{U}(\mathcal{V}_C)$	transmit vector at node i
Z_j	$\sim \mathcal{N}(0, I_n)$	AWGN at relay antenna j
Y_j	continuous	received vector at relay antenna j

APPENDIX

In this section we provide the proof of Theorem 1. An overview over all random variables is provided in Table I.

Proof: For the achievability of the secrecy rate region we must show that the following weak secrecy condition holds:

$$\lim_{n \rightarrow \infty} \frac{1}{n} I(\mathcal{W}; \mathcal{Y} \mid U_1, \dots, U_L) = 0, \quad (52)$$

for all $\mathcal{W} \in \mathcal{P}(\{W_1, \dots, W_L\})$ and all $\mathcal{Y} \in \mathcal{P}(\{Y_1, \dots, Y_{\eta_R}\})$ where $\mathcal{P}(X)$ is the power set of X . For the ease of readability we omit the condition on U_1, \dots, U_L in the following since the dither is present and known in every mutual information and entropy and does not change the equations. By using the chain rule for mutual information we see that¹

$$\begin{aligned} & I(W_1, \dots, W_L; Y_1, \dots, Y_{\eta_R}) - I(W_1, \dots, W_m; Y_1, \dots, Y_{\eta_R}) \\ &= \sum_{\ell=m}^L I(W_\ell; Y_1, \dots, Y_{\eta_R} \mid W_1, \dots, W_{\ell-1}). \end{aligned} \quad (53)$$

Because of the non-negativity of mutual information we have

$$\begin{aligned} & I(W_1, \dots, W_L; Y_1, \dots, Y_{\eta_R}) \\ & - I(W_1, \dots, W_m; Y_1, \dots, Y_{\eta_R}) \geq 0 \end{aligned} \quad (54)$$

¹Note that for $\ell = L$: $I(W_L; Y_1, \dots, Y_{\eta_R} \mid W_1, \dots, W_{L-1}) \neq 0$ because of the random binning.

and therefore

$$\begin{aligned} I(W_1, \dots, W_L; Y_1, \dots, Y_{\eta_R}) \\ \geq I(W_1, \dots, W_m; Y_1, \dots, Y_{\eta_R}), \quad \forall m < L. \end{aligned} \quad (55)$$

Using the symmetry of mutual information and the same arguments as above, we can show that

$$\begin{aligned} I(W_1, \dots, W_L; Y_1, \dots, Y_{\eta_R}) \\ \geq I(W_1, \dots, W_L; Y_1, \dots, Y_m), \quad \forall m < \eta_R. \end{aligned} \quad (56)$$

Hence, it is sufficient to show that

$$\lim_{n \rightarrow \infty} \frac{1}{n} I(W_1, \dots, W_L; Y_1, \dots, Y_{\eta_R}) = 0 \quad (57)$$

which implies (52). This condition is equivalent to

$$\begin{aligned} \lim_{n \rightarrow \infty} \frac{1}{n} H(W_1, \dots, W_L) \\ \leq \lim_{n \rightarrow \infty} \frac{1}{n} H(W_1, \dots, W_L \mid Y_1, \dots, Y_{\eta_R}). \end{aligned} \quad (58)$$

We can explicitly write the left hand side and get

$$L \cdot R_s \leq \lim_{n \rightarrow \infty} \frac{1}{n} H(W_1, \dots, W_L \mid Y_1, \dots, Y_{\eta_R}). \quad (59)$$

We now need a lower bound on the right hand side.

$$\lim_{n \rightarrow \infty} \frac{1}{n} H(W_1, \dots, W_L \mid Y_1, \dots, Y_{\eta_R}) \quad (60)$$

$$= \lim_{n \rightarrow \infty} \frac{1}{n} [H(W_1, \dots, W_L \mid X_1, \dots, X_L, Y_1, \dots, Y_{\eta_R}) + H(X_1, \dots, X_L \mid Y_1, \dots, Y_{\eta_R})] \quad (61)$$

$$- H(X_1, \dots, X_L \mid W_1, \dots, W_L, Y_1, \dots, Y_{\eta_R})] \stackrel{a)}{\geq} \lim_{n \rightarrow \infty} \frac{1}{n} [H(X_1, \dots, X_L \mid Y_1, \dots, Y_{\eta_R}) - n\delta(n)] \quad (62)$$

$$= \lim_{n \rightarrow \infty} \frac{1}{n} [H(X_1, \dots, X_L \mid Y_1, \dots, Y_{\eta_R}) - H(X_1, \dots, X_L) + H(X_1, \dots, X_L) - n\delta(n)] \quad (63)$$

$$= \lim_{n \rightarrow \infty} \frac{1}{n} [H(X_1, \dots, X_L) - I(X_1, \dots, X_L; Y_1, \dots, Y_{\eta_R}) - n\delta(n)] \quad (64)$$

$$\stackrel{b)}{\geq} L \cdot (R_s + R_d) - \frac{1}{2} \log_2 \det(I_{\eta_R} + PHH') \quad (65)$$

We have used the following arguments:

- a) We used Fano's inequality to bound the last term. This is because the size of each bin is kept small enough such that given W_1, \dots, W_L , the eavesdropper can determine X_1, \dots, X_L from the received signals.
- b) We note that the term $I(X_1, \dots, X_L; Y_1, \dots, Y_{\eta_R})$ corresponds to the mutual information of a MIMO channel. We rewrite the mutual information in terms of entropy, i.e.,

$$\begin{aligned} I(X_1, \dots, X_L; Y_1, \dots, Y_{\eta_R}) \\ = h(Y_1, \dots, Y_{\eta_R}) - h(Y_1, \dots, Y_{\eta_R} \mid X_1, \dots, X_L). \end{aligned} \quad (66)$$

We use the fact that the normal distribution maximizes the entropy for an average power constraint to get an upper bound on the first term. Furthermore, from [42, Section 3.2] we know that if X is distributed according to a normal distribution with zero-mean and covariance $E[xx'] = PI_L$ than $Y = HX + Z$ is also distributed according to a normal

distribution with zero-mean and covarianz $E[yy'] = PHH' + I_{\eta_R}$.

$$\begin{aligned}
h(Y_1, \dots, Y_{\eta_R}) &= h(Y_{1,1}, \dots, Y_{1,n}, \dots, Y_{\eta_R,1}, \dots, Y_{\eta_R,n}) \\
&= h(Y_{1,1}, \dots, Y_{\eta_R,1}, \dots, Y_{1,n}, \dots, Y_{\eta_R,n}) \\
&\leq \sum_{i=1}^n h(Y_{1,i}, \dots, Y_{\eta_R,i}) \\
&\leq n \cdot \frac{1}{2} \log_2((2\pi e)^L \det(PHH' + I_{\eta_R})).
\end{aligned}$$

The only uncertainty in the received signals Y_1, \dots, Y_{η_R} , if the transmitted signals X_1, \dots, X_L are given, comes from the noise Z_1, \dots, Z_{η_R} . The noise is i.i.d. with respect to a normal distribution which results in the following entropy:

$$\begin{aligned}
h(Y_1, \dots, Y_{\eta_R} \mid X_1, \dots, X_L) \\
&= h(Z_1, \dots, Z_{\eta_R}) \\
&= \sum_{i=1}^n h(Z_{1,i}, \dots, Z_{\eta_R,i}) \\
&= n \cdot h(Z_{1,i}, \dots, Z_{\eta_R,i}) \\
&= n \cdot \frac{1}{2} \log_2((2\pi e)^L \det(I_{\eta_R})).
\end{aligned}$$

Putting everything together results in

$$\begin{aligned}
I(X_1, \dots, X_L; Y_1, \dots, Y_{\eta_R}) \\
&\leq n \cdot \frac{1}{2} \log_2((2\pi e)^L \det(PHH' + I_{\eta_R})) \\
&\quad - n \cdot \frac{1}{2} \log_2((2\pi e)^L \det(I_{\eta_R})) \\
&= n \cdot \frac{1}{2} \log_2 \frac{(2\pi e)^L \det(PHH' + I_{\eta_R})}{(2\pi e)^L \det(I_{\eta_R})} \\
&= n \cdot \frac{1}{2} \log_2 \det(I_{\eta_R} + PHH').
\end{aligned}$$

Since all rates are symmetric and $R_s + R_d \leq R_{\text{CF}}$ we get the following weak secrecy rate

$$L \cdot R_s \leq L \cdot R_{\text{CF}} - \frac{1}{2} \log_2 \det(I_{\eta_R} + PHH'). \quad (67)$$

This concludes the proof. ■

REFERENCES

- [1] R. Ahlswede, N. Cai, S.-Y. R. Li, and R. W. Yeung, "Network information flow," *IEEE Transactions on Information Theory*, vol. 46, no. 4, pp. 1204–1216, 2000.
- [2] C. Fragouli and E. Soljanin, *Network Coding Fundamentals*. Now Publishers, 2007.
- [3] R. W. Yeung, *Information Theory and Network Coding*. Springer, 2008.
- [4] R. W. Yeung, S.-Y. R. Li, N. Cai, and Z. Zhang, *Network Coding Theory Part I: Single Source*. Now Publishers, 2005.
- [5] ———, *Network Coding Theory Part II: Multiple Source*. Now Publishers, 2005.
- [6] S. Katti, H. Rahul, W. Hu, D. Katabi, M. Médard, and J. Crowcroft, "XORs in the air: Practical wireless network coding," *IEEE/ACM Transactions on Networking*, vol. 16, no. 3, pp. 497–510, Jun. 2008.
- [7] S. Zhang, S. C. Liew, and P. P. Lam, "Hot topic: physical-layer network coding," in *Proc. of the Annual International Conference on Mobile Computing and Networking*, 2006.
- [8] B. Nazer and M. Gastpar, "Reliable physical layer network coding," *Proceedings of the IEEE*, vol. 99, no. 99, pp. 438–460, 2011.
- [9] ———, "Compute-and-forward: Harnessing interference through structured codes," *IEEE Transactions on Information Theory*, vol. 57, no. 10, pp. 6463–6486, 2011.
- [10] U. Erez and R. Zamir, "Achieving $\frac{1}{2} \log(1 + \text{SNR})$ on the AWGN channel with lattice encoding and decoding," *IEEE Transactions on Information Theory*, vol. 50, no. 10, pp. 2293–2314, 2004.
- [11] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.
- [12] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 339–348, 1978.
- [13] J. Huang, A. Mukherjee, and A. L. Swindlehurst, "Secure communication via an untrusted non-regenerative relay in fading channels," *IEEE Transactions on Signal Processing*, vol. 61, no. 10, pp. 2536–2550, May 2013.
- [14] X. He and A. Yener, "Cooperation with an untrusted relay: A secrecy perspective," *IEEE Transactions on Information Theory*, vol. 56, no. 8, pp. 3807–3827, Aug. 2010.
- [15] ———, "Strong secrecy and reliable byzantine detection in the presence of an untrusted relay," *IEEE Transactions on Information Theory*, vol. 59, no. 1, pp. 177–192, 2013.
- [16] ———, "End-to-end secure multi-hop communication with untrusted relays," *IEEE Transactions on Wireless Communications*, vol. 12, no. 1, pp. 1–11, Jan. 2013.
- [17] E. Tekin and A. Yener, "The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2735–2751, 2008.
- [18] ———, "Correction to: The general Gaussian multiple access and two-way wire-tap channels: Achievable rates and cooperative jamming," *IEEE Transactions on Information Theory*, vol. 56, no. 9, pp. 4762–4763, 2010.
- [19] A. J. Pierrot and M. R. Bloch, "Strongly secure communications over the two-way wiretap channel," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 595–605, 2011.

- [20] L.-C. Choo, C. Ling, and K.-K. Wong, "Achievable rates for lattice coded Gaussian wiretap channels," in *IEEE International Conference on Communications Workshops (ICC)*, Jun. 2011, pp. 1–5.
- [21] F. Oggier, P. Solé, and J.-C. Belfiore, "Lattice codes for the wiretap Gaussian channel: Construction and analysis," Jan. 2013, submitted to *IEEE Transactions on Information Theory*. [Online]. Available: <http://arxiv.org/abs/1103.4086>
- [22] J.-C. Belfiore and F. Oggier, "Secrecy gain: A wiretap lattice code design," in *International Symposium on Information Theory and its Applications (ISITA)*, Oct. 2010, pp. 174–178.
- [23] C. Ling, L. Luzzi, and J.-C. Belfiore, "Lattice codes achieving strong secrecy over the mod- Λ Gaussian channel," in *Proc. of the International Symposium on Information Theory (ISIT)*, 2012, pp. 2306–2310.
- [24] C. Ling, L. Luzzi, J.-C. Belfiore, and D. Stehlé, "Semantically secure lattice codes for the Gaussian wiretap channel," Oct. 2012. [Online]. Available: <http://arxiv.org/abs/1210.6673>
- [25] J.-C. Belfiore, "Lattice codes for the compute-and-forward protocol: The flatness factor," in *IEEE Information Theory Workshop (ITW)*, Oct. 2011, pp. 1–4.
- [26] N. Kashyap, S. V. V. and A. Thangaraj, "Secure compute-and-forward in a bidirectional relay," 2012. [Online]. Available: <http://arxiv.org/abs/1206.3392>
- [27] X. He and A. Yener, "Providing secrecy with lattice codes," in *46th Annual Allerton Conference on Communication, Control, and Computing*, 2008, pp. 1199–1206.
- [28] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*, 3rd ed. Springer, 1999.
- [29] R. Zamir, "Lattices are everywhere," in *Information Theory and Applications Workshop*, 2009, pp. 392–421.
- [30] U. Erez, S. Litsyn, and R. Zamir, "Lattices which are good for (almost) everything," *IEEE Transactions on Information Theory*, vol. 51, no. 10, pp. 3401–3416, 2005.
- [31] D. Tse and P. Viswanath, *Fundamentals of Wireless Communication*. Cambridge University Press, 2005.
- [32] J. Zhan, B. Nazer, U. Erez, and M. Gastpar, "Integer-forcing linear receivers," in *IEEE International Symposium on Information Theory Proceedings (ISIT)*. IEEE, 2010, pp. 1022–1026.
- [33] J. Richter, C. Scheunert, and E. A. Jorswieck, "An efficient branch-and-bound algorithm for compute-and-forward," in *Proc. of the 23rd IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC'12)*, 2012.
- [34] L. Wei and W. Chen, "Compute-and-forward network coding design over multi-source multi-relay channels," *IEEE Transactions on Wireless Communications*, vol. 11, no. 9, pp. 3348–3357, 2012.
- [35] R. Mochaourab and E. A. Jorswieck, "Optimal beamforming in interference networks with perfect local channel information," *IEEE Transactions on Signal Processing*, vol. 59, no. 3, pp. 1128–1141, 2011.
- [36] M. P. Wilson, K. Narayanan, H. D. Pfister, and A. Sprintson, "Joint physical layer coding and network coding for bidirectional relaying," *IEEE Transactions on Information Theory*, vol. 56, no. 11, pp. 5641–5654, Nov. 2010.
- [37] S. Zhang and S.-C. Liew, "Channel coding and decoding in a relay system operated with physical-layer network coding," *IEEE Journal on Selected Areas in Communications*, vol. 27, no. 5, pp. 788–796, Jun. 2009.
- [38] P. Popovski and H. Yomo, "Physical network coding in two-way wireless relay channels," in *IEEE International Conference on Communications (ICC)*, Jun. 2007, pp. 707–712.

- [39] A. El Gamal, O. O. Koyluoglu, M. Youssef, and H. El Gamal, "Achievable secrecy rate regions for the two-way wiretap channel," *IEEE Transactions on Information Theory*, vol. 59, no. 12, pp. 8099–8114, Dec. 2013.
- [40] M. R. Bloch and J. N. Laneman, "Strong secrecy from channel resolvability," *IEEE Transactions on Information Theory*, vol. 59, no. 12, pp. 8077–8098, Dec. 2013.
- [41] X. He and A. Yener, "Providing secrecy with structured codes: Two-user Gaussian channels," *IEEE Transactions on Information Theory*, vol. 60, no. 4, pp. 2121–2138, Apr. 2014.
- [42] E. Telatar, "Capacity of multi-antenna Gaussian channels," *European Transactions on Telecommunications*, vol. 10, no. 6, pp. 585–595, 1999.